

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-252654

(43)Date of publication of application : 06.09.2002

(51)Int.Cl.

H04L 12/66
G06F 13/00

(21)Application number : 2001-048083

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 23.02.2001

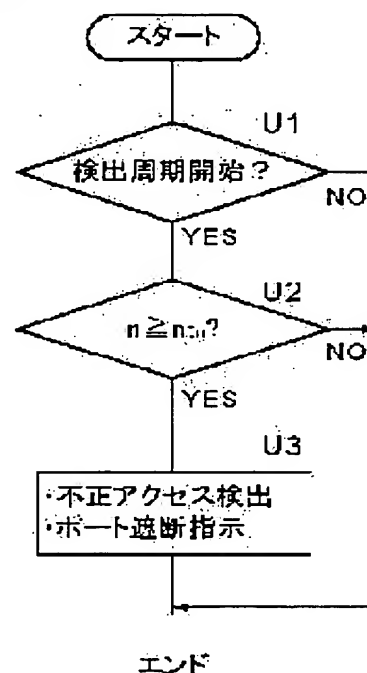
(72)Inventor : KINOSHITA YOSUKE

(54) INTRUSION DETECTION DEVICE, SYSTEM, AND ROUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an intrusion detection device capable of detecting an unauthorized access intrusion such as DDoS(distributed denial of service) attack automatically with high accuracy.

SOLUTION: An intrusion detection unit of a router acquires from a communication route a packet which reaches at the router, and generates a structure corresponding to each session based on network layer data and transport layer data described in the header of the packet. This structure is discarded when the session is terminated normally. The intrusion detection unit inspects the total number n of structures for each prescribed period. If there is any structure with a prescribed threshold n_{th} or more as a result of the inspection, the unit detects it as the unauthorized access intrusion occurrence. Since a structure is generated for each session and the presence/absence of the unauthorized access intrusion is detected, based on the number of the generated structures, a DDoS attack, which establishes a large volume of different sessions, can be detected automatically with high accuracy.



LEGAL STATUS

[Date of request for examination]

21.10.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-252654

(P2002-252654A)

(43) 公開日 平成14年9月6日(2002.9.6)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 9
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 C 5 K 0 3 0

審査請求 未請求 請求項の数11 O L (全 22 頁)

(21) 出願番号 特願2001-48083(P2001-48083)

(22) 出願日 平成13年2月23日(2001.2.23)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 木下 洋輔

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外1名)

Fターム(参考) 5B089 GA31 GB02 HB18 HB19 KA17

KB13 KC47 KC03 KG10 MC01

5K030 GA15 HA08 HC01 HD03 KA01

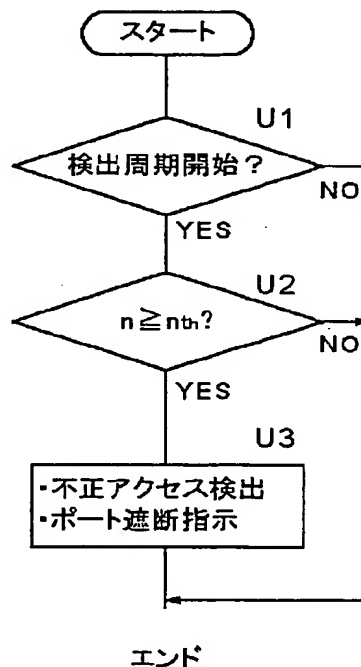
KA05 KA13

(54) 【発明の名称】 侵入検出装置およびシステムならびにルータ

(57) 【要約】

【課題】 DDoS攻撃などの不正アクセスの侵入を自動的にかつ高精度に検出できる侵入検出装置を提供する。

【解決手段】 ルータの侵入検出部は、ルータに到達するパケットを通信路から取得し、当該パケットのヘッダに記述されているネットワーク層(IP層)およびトランスポート層(TCP層)のデータに基づいてセッションごとに対応する構造体を生成する。この構造体は、セッションが正常終了した場合に破棄される。侵入検出部は、所定の検査周期ごとに、構造体の総数 n を検査する。その結果、所定の不正検出しきい値 n_{th} 以上の構造体があれば、不正アクセスの侵入があると検出する。セッションごとに構造体を生成してその数に基づいて不正アクセスの侵入の有無を検出するから、大量の異なるセッションを確立するDDoS攻撃を自動的にかつ精度良く検出できる。



【特許請求の範囲】

【請求項1】 コンピュータネットワーク上に確立されるセッションを介して伝送されるパケットを取得し、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて上記セッションごとに対応する構造体を生成し、当該構造体が異常な数となる場合に、不正アクセスの侵入を検出する侵入検出装置。

【請求項2】 コンピュータネットワーク上に確立されるセッションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セッションごとに対応する構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、不正アクセスの侵入を検出する検出手段とを含む侵入検出装置。

【請求項3】 請求項2において、さらに、セッションが正常終了した場合に、当該セッションに対応する構造体を破棄する構造体破棄手段を含む侵入検出装置。

【請求項4】 請求項3において、構造体生成手段は、上記取得されたパケット自体を構造体の一部として構造体を生成するものであり、

上記構造体の一部であるパケットを結合するパケット結合手段と、

このパケット結合手段によるパケット結合の結果パケットを正常に結合できなかった時点において、当該構造体の保留を決定する保留決定手段とをさらに含み、

上記構造体破棄手段は、上記パケット結合手段によるパケット結合の結果パケットを正常に結合することができた場合に、当該セッションに対応する構造体を破棄するものである侵入検出装置。

【請求項5】 請求項4において、パケット結合手段は、一連のパケットをすべて取得した後にパケットを結合する、または、パケットを取得するたびにパケットを結合するものである侵入検出装置。

【請求項6】 複数の侵入検出装置およびこれら複数の侵入検出装置に接続された上位管理装置を含む侵入検出システムにおいて、

上記複数の侵入検出装置は、それぞれ、

コンピュータネットワーク上に確立されるセッションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セッションごとに対応する

構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、上記上位管理装置に対して不正アクセス検出信号を送信する信号送信手段と、

上位管理装置から送信されてきた判定信号に基づいて、不正アクセスの侵入の有無を検出する検出手段とを有するものであり、

上記上位管理装置は、上記複数の侵入検出装置のすべてから上記不正アクセス検出信号を受信したか否かを判別する受信判別手段と、

この受信判別手段によりすべての侵入検出装置から不正アクセス検出信号を受信したと判別された場合に不正アクセスの侵入があることを示し、上記受信判別手段によりすべての侵入検出装置から不正アクセス検出信号を受信していないと判別された場合に不正アクセスの侵入がないことを示す上記判定信号を少なくとも不正アクセス検出信号を送信してきた侵入検出装置に対して送信する判定信号送信手段とを有するものである侵入検出システム。

【請求項7】 複数の侵入検出装置を含む侵入検出システムにおいて、

上記複数の侵入検出装置は、それぞれ、

コンピュータネットワーク上に確立されるセッションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セッションごとに対応する構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、他の侵入検出装置に対してアクセス状況を確認するアクセス状況確認信号を送信するアクセス状況確認手段と、

他の侵入検出装置からアクセス状況確認信号を受信した場合に、上記構造体生成手段により生成される構造体の数を含む返信信号を上記他の侵入検出装置に返信する返信手段と、

他の侵入検出装置から返信されてきた返信信号に含まれている構造体の数に基づいて、不正アクセスの侵入の有無を検出する検出手段とを有するものである侵入検出システム。

【請求項8】 請求項7において、上記複数の侵入検出装置は、さらに、上記不正検出しきい値の補正值である補正しきい値を記憶する補正しきい値記憶手段と、他の

侵入検出装置からアクセス状況確認信号を受信した場合に、上記不正検出しきい値を上記補正しきい値記憶手段に記憶されている補正しきい値に補正するしきい値補正手段とをそれぞれ有するものである侵入検出システム。

【請求項9】 請求項2ないし5のいずれかにおいて、さらに、上記パケット取得手段により取得されたパケットのヘッダに記述されているトランスポート層のデータに基づいて、対象サービスに対応するパケットであるかを判別するサービス種別判別手段を含み、

上記構造体生成手段は、上記サービス種別判別手段により取得されたパケットが対象サービスに対応するパケットであると判別された場合にのみ、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、セッションごとに対応する構造体を生成するものである侵入検出装置。

【請求項10】 請求項9に記載された侵入検出装置とおとりサーバを含む侵入検出システムにおいて、上記侵入検出装置は、さらに、上記サービス種別判別手段により取得されたパケットが対象サービスに対応するパケットでないと判別された場合に、当該パケットをコピーし、当該コピーされたパケットを上記おとりサーバに転送する手段を有し、

上記おとりサーバは、上記パケットを受信した場合に、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、セッションごとに対応する構造体を生成する構造体生成手段と、この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上になったかを判別する判別手段と、

この判別手段により上記不正検出しきい値以上になったと判別された場合に、不正アクセスの侵入を検出する検出手段とを含む不正アクセス検出手段とを有するものである侵入検出システム。

【請求項11】 パケットを中継するルータにおいて、請求項1ないし5のいずれかまたは請求項9の侵入検出装置と、この侵入検出装置により不正アクセスの侵入が検出された場合に、パケット中継を自動的に禁止する手段とを含むルータ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、分散サービス不能攻撃（DDoS attack、DDoS: Distributed - denial of service）および分散ポートスキャン攻撃などの不正アクセスの侵入を検出する侵入検出装置およびシステム、ならびに上記侵入検出装置が用いられたルータに関する。

【0002】

【従来の技術】従来から、DoS攻撃などの不正アクセスの侵入を検出する侵入検出装置（IDS: Intrusion

Detection System）が知られている。DoS攻撃は、侵入者のコンピュータから攻撃対象のコンピュータに大量のパケットを短時間で送信し、攻撃対象のコンピュータのシステムリソースを費やさせることにより、当該コンピュータをダウンさせる行為のことである。

【0003】上記の侵入検出装置は、そのような攻撃からコンピュータを保護すべく、たとえばルータに備えられ、通信路上を流れ当該ルータに到達する直前のパケットを取得し、当該パケットのヘッダに記述されている送信先ポートまたは送信元ポートに基づいてアクセス量を監視することにより、不正アクセスの侵入を検出している。より具体的には、パケットには、送信先ポートおよび送信元ポートを記述したヘッダが含まれている。侵入検出装置は、当該パケットヘッダから送信先ポートおよび送信元ポートを抽出し、たとえば1つの送信元から1つの送信先へのパケット量が異常に多い場合などに、不正アクセスであると検出する。なお、このような侵入検出装置は、一般にネットワーク型IDSと呼ばれている。

【0004】

【発明が解決しようとする課題】ところで、最近では、複数の送信元から攻撃対象の送信先へ一斉にパケットを送信するDDoS攻撃と言われるものがある。より具体的には、DDoS攻撃は、侵入者のコンピュータから第3者のコンピュータに対してエージェントと呼ばれるソフトウェアを通信網を介してインストールし、そのエージェントをリモート操作することにより攻撃対象のコンピュータに多くのパケットを送信させ、攻撃対象のコンピュータのシステムリソースを費やさせることにより当該コンピュータをダウンさせる行為のことである。

【0005】このDDoS攻撃においては、第3者のコンピュータが送信元となるため、到着するパケットのヘッダに含まれる送信元ポートは、異なる複数のものとなる。したがって、侵入検出装置は、大量のパケットが到着しても、単なるアクセス量の増加であると判断する可能性がある。そのため、従来の侵入検出装置では、DDoS攻撃などの不正アクセスを良好に検出することができないとの問題があった。なお、不正アクセスであるかは、コンピュータがダウンした後管理者が手作業でログ解析などを行って初めて判明するものであり、システムダウンと合わせて非常に非効率的な作業をしなければならなかった。

【0006】そこで、本発明の目的は、DDoS攻撃などの不正アクセスの侵入を自動的にかつ高精度に検出できる侵入検出装置およびシステムを提供することである。

【0007】また、本発明の他の目的は、上記侵入検出装置を用いることにより、不正アクセス侵入による被害拡大を迅速に防止できるルータを提供することである。

【0008】

【課題を解決するための手段】上記目的を達成するためのこの発明は、コンピュータネットワーク上に確立されるセッションを介して伝送されるパケットを取得し、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて上記セッションごとに対応する構造体を生成し、当該構造体が異常な数となる場合に、不正アクセスの侵入を検出するものである。

【0009】

【発明の実施の形態】以下では、本発明の実施の形態を、添付図面を参照して詳細に説明する。

【0010】実施の形態1

図1は、本発明の実施の形態1に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。このコンピュータネットワークは、インターネットなどの外部ネットワーク1と、当該外部ネットワーク1に対してパケットを中継するルータ2を介して接続され、企業などの組織内に構築された内部ネットワーク3とを有するものである。

【0011】外部ネットワーク1には、複数のコンピュータ4が接続されている。この外部ネットワーク1のコンピュータ4は、代表的には、パーソナルコンピュータおよびワークステーションである。内部ネットワーク3には、複数のコンピュータ5が接続されている。この内部ネットワーク3のコンピュータ5は、代表的には、パーソナルコンピュータ、メールサーバ、ウェブサーバおよびFTP(File Transfer Protocol)サーバである。

【0012】外部および内部ネットワーク1、3の各コンピュータ4、5は、TCP/IP(Transmission Control Protocol / Internet Protocol)を通信プロトコルとして使用し、パケットを送受信する機能を有している。ここに、TCPは、OSI(Open Systems Interconnection)参照モデルにおけるトランスポート層の通信プロトコルであり、IPは、OSI参照モデルにおけるネットワーク層の通信プロトコルである。なお、通信プロトコルは、TCP/IPに限定されるものでなく、ARP(Address Resolution Protocol)、RARP(Reverse Address Resolution Protocol)、IPX(Internet Network Packet Protocol)、NetBIOS(Network Basic Input Output System)、ICMP(Internet Control Message Protocol)、IGMP(Internet Group Management Protocol)、SPX(Sequenced Packet Exchange)、NCP(Network Control Protocol)、RIP(Routing Information Protocol)、NLSP(Network Link Service Protocol)、SAP(Service Advertising Protocol)などの他の通信プロトコルでもよいことはもちろんである。

【0013】各コンピュータ4、5は、正常なパケット通信を実行する場合、トランスポート層の通信プロトコルであるTCPに従って相手方コンピュータとの間でセッションを確立し、信頼性のあるパケット通信を実現す

る。より具体的には、発呼側および着呼側のコンピュータ間でいわゆる3ウェイハンドシェイクが実行されることによりセッション(論理的通信路)が確立される。

【0014】さらに具体的には、発呼側のコンピュータは、回線接続要求パケットを着呼側のコンピュータに対して送信する。着呼側のコンピュータは、当該回線接続要求に対して接続応答パケットを返信する。この際、着呼側のコンピュータは、これから確立しようとしているセッションを識別する情報としてセッション識別子を発呼側のコンピュータに割り当てる。

【0015】これに応答して、発呼側のコンピュータは、パスワード等の通信に必要なデータを含むパケットを着呼側のコンピュータに返信する。このとき、発呼側のコンピュータは、上記着呼側のコンピュータから割り当てられたセッション識別子を上記パケットのヘッダに記述する。着呼側のコンピュータは、上記通信に必要なデータを受け取ると、発呼側のコンピュータに対して通信許可パケットを通知する。こうして、セッションが確立する。

【0016】以後、発呼側のコンピュータからパケットを送信する際には、上記割り当てられたセッション識別子をヘッダに記述する。すなわち、セッションを正常に確立しようとしそれが実際に確立されれば、着呼側のコンピュータには、発呼側のコンピュータから同一のセッション識別子を有する複数のパケットが送信されてくることになる。

【0017】一方、不正アクセス時には、発呼側のコンピュータにインストールされているエージェントと呼ばれる不正ツールは、通常、着呼側のコンピュータとの間で正常なセッションを確立しようとすることなく、一方的にパケットを着呼側のコンピュータに対して送信し続ける。この場合、パケットのヘッダには、通常、適当なセッション識別子が記述される。したがって、不正アクセス時には、複数の異なるセッション識別子をそれぞれ有する複数のパケットが不正アクセス元のコンピュータから着呼側のコンピュータに送信されることになる。

【0018】なお、上述のように、不正アクセス時には正常な意味でのセッションは確立されていないけれども、本実施の形態1においては、パケットを着呼側のコンピュータに送り込む論理的な通信路が形成されているという意味において、セッションが確立されているとみなすこととしている。

【0019】本実施の形態1に係るルータ2は、不正アクセス時には複数の異なるセッション識別子をそれぞれ有するパケットが送信されてくることに着目し、セッション識別子ごとに、すなわちセッションごとに、そのセッションに関する情報を記述する構造体を生成し、当該構造体が異常な数になった場合に、不正アクセスの侵入を検出している。より具体的には、ルータ2は、コンピュータネットワーク上に確立されたセッションを介して伝送されて

10

20

30

40

50

いるバケットを取得する。言い替えば、ルータ2は、通信路上を流れているバケットを取得する。その後、ルータ2は、各セッションに対応する構造体を生成して保持し、当該構造体の総数が所定の不正検出しきい値 n_{th} 以上になった場合に、不正アクセスの侵入を検出する。ここに、構造体を構成するセッションに関する情報とは、送信元IPアドレス、送信先IPアドレス、送信元ポートおよび送信先ポートなどのセッション基本情報、ならびに最終バケット到着時刻および総バケット数などのセッション拡張情報である。

【0020】ただし、アクセス量の増加に伴って正常なセッションが大量に確立される場合もあり、この場合上記構造体もそのセッションの数に応じて生成されることになるから、上述の判断基準のみでは、正常なアクセスを不正アクセスと誤検出するおそれがある。

【0021】そこで、本実施の形態1に係るルータ2は、正常なセッションに対応する構造体については所定の破棄条件を満足したことに応じて破棄することとしている。上記所定の破棄条件は、正常なセッションに対してのみ該当する条件である。たとえば、上記所定の破棄条件は、セッションが正常に終了したことである。セッションが正常に終了したか否かは、たとえば、セッション開始時刻、最終バケット到着時刻および総バケット数などのセッション拡張情報を参照し、比較的短時間で一連のバケットをすべて受信したか否かにより判断できる。したがって、残っていく構造体のほとんどは、不正アクセスに対応するものとなる。そのため、構造体の数を見るだけでも、正常なアクセスを不正アクセスと誤検出することを防止できる。

【0022】しかも、セッションが正常に確立しているか否かを反映する構造体を参照して不正アクセスの検出を行っているから、従来のように送信先ポートおよび送信元ポートを監視するだけでは困難であったDDoS攻撃を自動的にかつ高精度に検出することができる。

【0023】図2は、バケットの構成を示す概念図である。バケットは、ヘッダおよびデータを含む。ヘッダは、たとえば、ネットワーク層およびトランスポート層など複数の通信プロトコル層のデータを有している。具体的には、ヘッダには、送信元IPアドレス、送信先IPアドレス、バケット長および1つのセッションに固有のセッション識別子がネットワーク層のデータとして記述されている。また、ヘッダには、送信元ポート、送信先ポート、バケットの送信順序を表しているシーケンス番号がネットワーク層のデータとして記述されている。

【0024】さらに、ヘッダには、たとえば、次バケットのバケット長が図2におけるビットフラグおよびフラグメントオフセットに記述されている。また、最後のシーケンス番号に対応するバケットのヘッダには、たとえば、最後のバケットであることを示す最終バケットデータが図2におけるビットフラグに記述されている。さら

に、ヘッダには、当該一連のバケットの総数が図2におけるビットフラグに記述されている。

【0025】図3は、ルータ2の内部構成を示すブロック図である。ルータ2は、上述のように、外部ネットワーク1からのアクセスを監視し、不正アクセスの侵入を検出した場合、以後の内部ネットワーク3への侵入を拒絶する機能を有している。より具体的には、ルータ2は、ルーティング部10および侵入検出部11を備えている。

10 【0026】ルーティング部10は、外部ネットワーク1から通信路12上を流れルータ2に到達するバケットを内部ネットワーク3に中継したり、内部ネットワーク3から出力されるバケットを外部ネットワーク1に中継したりする。この場合、ルーティング部10は、侵入検出部11の検出結果を参照して中継処理を実行する。

20 【0027】侵入検出部11は、ルータ2に到達するバケットのヘッダを監視することにより不正アクセスの侵入を検出する。より具体的には、侵入検出部11は、しきい値記憶部11aおよび構造体記憶部11bを有している。しきい値記憶部11aは、上記不正検出しきい値 n_{th} を記憶するものである。不正検出しきい値 n_{th} は、当該ルータの管理者が任意に設定できるものであり、たとえば、これ以上の数であればアクセス量の増加が異常であると考えられる値に設定される。構造体記憶部11bは、上記構造体を記憶するものである。

30 【0028】侵入検出部11は、ルータ2に到達するすべてのバケットを取得し、当該バケットのヘッダを抽出し、セッションを識別する。侵入検出部11は、この識別されたセッションに従って構造体を生成し、上記構造体記憶部11bに記憶させる。侵入検出部11は、この構造体記憶部11bに記憶されている構造体の総数 n が上記しきい値記憶部11aに記憶されている不正検出しきい値 n_{th} 以上であるか否かに基づいて、不正アクセスの侵入の有無を検出する。もしも不正アクセスの侵入を検出した場合、侵入検出部11は、ルーティング部10にアクセスし、外部ネットワーク1に繋がっている接続ポートを封鎖する。こうして、不正アクセスの被害から内部ネットワーク3を保護している。

40 【0029】侵入検出部11は、たとえば、ルータ2に実装されるコンピュータボードである。より具体的には、当該コンピュータボードは、コンピュータプログラムを記憶しているIC(Integrated Circuit)およびメモリを搭載するものであり、上記コンピュータプログラムの1つは、不正アクセス検出プログラムである。すなわち、より詳細に見れば、侵入検出部11は、上記不正アクセス検出プログラムを記憶しているICおよびメモリである。

50 【0030】図4は、構造体を示す概念図である。上述のように、構造体は、セッションごとに生成されるものである。構造体は、各セッションごとに、セッション基本情報

およびセッション拡張情報を含む。セッション基本情報は、送信元IPアドレスおよび送信先IPアドレス、セッション識別子などのネットワーク層の情報と、送信元ポートおよび送信先ポートなどのトランスポート層のデータと、論理的に隣接する構造体のアドレスを記述するセッション情報ディスクリプタポイントと、対応するセッション拡張情報のアドレスを記述する次ディスクリプタとを有する。セッション拡張情報は、IPセッション開始時刻と、TCPセッション開始時刻と、最終パケット到着時刻と、侵入検出部11により取得されたパケットの総数である総パケット数とを有する。なお、連鎖構造の最後の構造体における次ディスクリプタポイントには、ヌル(NUL)値が記述される。

【0031】図5、図6および図7は、侵入検出部11において実行される不正アクセス検出処理を説明するためのフローチャートである。不正アクセス検出処理は、複数の処理から構成されている。具体的には、不正アクセス検出処理は、構造体生成/破棄処理、構造体破棄処理および構造体数検査処理からなる。

【0032】図5は、構造体生成/破棄処理を説明するためのフローチャートである。侵入検出部11は、ルータ2に到達するパケットを通信路12から取得し(ステップS1)、当該パケットからヘッダを抽出する(ステップS2)。その後、侵入検出部11は、当該ヘッダ中のセッション識別子に基づいて、構造体を生成する(ステップS3～S5)。

【0033】より具体的には、侵入検出部11は、参照されたセッション識別子と同じセッション識別子の構造体が構造体記憶部11bに記憶されているか否かを検索する(ステップS3)。同じセッション識別子の構造体があれば(ステップS3のYES)、侵入検出部11は、当該構造体を更新する(ステップS4)。より具体的には、侵入検出部11は、最終パケット到着時刻および総パケット数を更新する。一方、同じセッション識別子の構造体がない(ステップS3のNO)、侵入検出部11は、当該セッション識別子に対応する構造体を新たに生成する(ステップS5)。すなわち、侵入検出部11は、図4に示されたような構造体を生成し、当該構造体を構造体記憶部11bに記憶させる。

【0034】また、侵入検出部11は、取得されたパケットのヘッダに最終パケットであることが記述されているか否かを判別する(ステップS6)。最終パケットでなければ(ステップS6のNO)、侵入検出部11は、当該処理を終了する。一方、最終パケットであれば(ステップS6のYES)、侵入検出部11は、当該最終パケットのヘッダに記述されている総パケット数と構造体に記述している総パケット数とを比較し、一致しているか否かを判別する(ステップS7)。一致していなければ(ステップS7のNO)、途中のシーケンス番号に対応するパケットの到着が遅れている可能性があるため、

侵入検出部11は、構造体の破棄を一時的に保留する(ステップS8)。一方、一致していれば(ステップS7のYES)、一連のパケットをすべて受信しセッションが正常に終了したものと考えられるから、侵入検出部11は、当該セッションに対応する構造体を破棄する(ステップS9)。

【0035】上述のように、侵入検出部11は、一連のパケットをすべて受信した場合にセッションが正常に終了したものととして、当該セッションに対応する構造体を破棄する。しかし、最終パケットの受信を確認したのに途中のパケットが遅れているためだけに構造体を一時保留し破棄できない場合がある。そこで、侵入検出部11は、このような構造体を確実に破棄すべく、上記構造体生成/破棄処理と並列に、図6に示された構造体破棄処理を実行する。

【0036】構造体破棄処理を実行する場合、侵入検出部11は、一定周期ごとに、構造体をスキャンする。より具体的には、侵入検出部11は、一定周期が開始されたことに応答して(ステップT1のYES)、1つ目の構造体を対象とし(ステップT2)、当該構造体中のセッション拡張情報の1つである最終パケット到着時刻を参照し、最終パケットが到着してから一定時間以上経過しているか否かを判別する(ステップT3)。さらに具体的には、侵入検出部11は、最終パケット到着時刻と現在時刻とを比較し、上記一定時間以上経過しているか否かを判別する。上記一定時間は、管理者が任意に設定可能なもので、たとえば1日、3日、1週間などである。

【0037】上記一定時間以上経過していれば、たとえば、発呼側のコンピュータで不具合が発生した、あるいは経由サーバで不具合が発生した、などが考えられる。しかも、不正アクセスでシステムダウンするのは短時間に大量のパケットが到着することを鑑みれば、最終パケット到着から時間が経過しているようなアクセスを不正アクセスとして検出する必要性はないと考えられる。そのため、上記一定時間以上経過していれば(ステップT3のYES)、侵入検出部11は、当該セッションに対応する構造体を破棄する(ステップT4)。

【0038】一方、一定時間以上経過していなければ(ステップT3のNO)、パケットの送信途中であると考えられるから、侵入検出部11は、すべての構造体についてのスキャンが終了したか否かを判別する(ステップT5)。すべての構造体についてのスキャンが終了していなければ(ステップT5のNO)、侵入検出部11は、次の構造体を対象とし(ステップT6)、上記ステップT3の処理に移行する。一方、すべての構造体についてのスキャンが終了していれば(ステップT5のYES)、侵入検出部11は、当該処理を終了する。

【0039】以上の処理により、侵入検出部11は、正常なセッションに対応する構造体については随時破棄していくことになる。したがって、残っていくのは、不正ア

クセスに対応する構造体ということになる。一方、DDoS攻撃のような不正アクセスは、上述のように、大量の不正なセッションを通して大量のバケットを送信し続けるから、残っている構造体の数が多ければ、不正アクセスであることを検出することができる。そこで、侵入検出部11は、上記構造体生成/破棄処理および構造体破棄処理と並列に、図7に示された構造体数検出処理を実行する。

【0040】侵入検出部11は、保有している構造体の数を一定の検出周期 Δt ごとに検査する。より具体的には、侵入検出部11は、上記検出周期 Δt の開始にตอบสนองして（ステップU1のYES）、保有している構造体の総数 n が不正検出しきい値 n_{th} 以上であるか否かを判別する（ステップU2）。構造体の総数 n が上記不正検出しきい値 n_{th} 未満であれば（ステップU2のNO）、不正アクセスの侵入はないと考えられるから、侵入検出部11は、当該処理を終了する。一方、構造体の総数 n が不正検出しきい値 n_{th} 以上であれば（ステップU2のYES）、DDoS攻撃を含む不正アクセスの侵入があると考えられるから、侵入検出部11は、ルーチング部10にアクセスし、外部ネットワーク1との接続ポートを遮断させる（ステップU3）。

【0041】以上のようにこの実施の形態1によれば、バケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいてセッションごとに対応する構造体を生成し、当該構造体の数が異常になれば、不正アクセスであると検出している。したがって、第三者のコンピュータにエージェントをインストールし単なるアクセス量の増加であると誤認させようとDDoS攻撃を仕掛けても、当該DDoS攻撃を自動的にかつ高精度に検出することができる。そのため、従来よりもセキュリティ信頼度が向上されたシステム構築を実現することができる。

【0042】また、正常アクセスに対応する構造体を確実に破棄しているから、構造体の総数に占めるDDoS攻撃などの不正アクセスに対応する構造体の比率を高くすることができる。したがって、単なるアクセス量増加を不正アクセスであると誤検出する頻度を大幅に低減できる。そのため、不正アクセスを一層高精度に検出することができる。

【0043】実施の形態2

上記実施の形態1では、セッションが正常に終了したか否かに基づいて、構造体を保留するか否かを判別している。これに対して、本実施の形態2では、セッションが正常に終了したか否かだけでなく一連のバケットを正常に結合できるか否かに基づいて、構造体を保留するか否かを判別することとしている。

【0044】セッションが正常に終了したか否かは、比較的短時間で一連のバケットをすべて受信したか否かに基づいて判断される。すなわち、最終バケットのヘッダに

記述されている最終バケットデータおよび総バケット数に基づいて判断される。しかし、ヘッダの書き換えは相対的に容易に行えるため、厳密に言えば、不正アクセスであってもセッションが正常に終了する場合がある。したがって、不正アクセスであるにもかかわらず、正常アクセスであると誤検出するおそれがある。一方、バケット長を変えたりすることは相対的に困難であるため、不正アクセスであればバケットを正常に結合することはできない。そこで、本実施の形態2では、バケットを正常に結合できるか否かに基づいて、構造体を保留するか否かを判別することとしている。

【0045】さらに具体的には、正常な通信ツールから送信された複数のバケットであれば、侵入検出部11において正常に結合することができる。より具体的には、正常なツールは、RFCに従って一連のデータを単純に複数のバケットに分割するだけなので、あるバケットのヘッダに記述されている次バケットに関するデータと実際に受信されるバケットとの間には整合性がある。たとえば、次バケットは数バイトのバケット長を有するとのデータがヘッダに記述されている場合、シーケンス番号から見た次バケットは確かにヘッダに記述されているのと同じバケット長を有している。したがって、侵入検出部11は、バケットを正常に結合することができる。

【0046】一方、不正ツールは攻撃対象のコンピュータにバケットを送り込むためのものであり上記RFCに従ってバケット生成を行っていないので、各バケットのヘッダに記述されている次バケットに関するデータと実際に受信されるバケットの間には、通常、整合性はない。したがって、たとえば次バケットは k バイトのバケット長を有するとのデータがヘッダに記述されている場合、シーケンス番号では次バケットでも上記 k バイトとは異なる i バイトのバケット長を有していることがある。そのため、バケットを正常に結合することができなくなる。

【0047】図8は、本実施の形態2に係る構造体を示す概念図である。この構造体は、セッション基本情報およびセッション拡張情報に加えて、バケット自体を到着バケット情報をその一部とする。到着バケット情報は、ヘッダおよびデータの両方を含むバケット自体と、当該バケットの到着時刻と、直後に取得された到着バケット情報の先頭アドレスを指示する次バケットディスクリプタポインタとを含む。セッション拡張情報は、到着バケット情報の先頭アドレスを指示する未生成バケット格納ディスクリプタポインタを有している。

【0048】図9は、本実施の形態2に係る構造体生成/破棄処理である。すなわち、本実施の形態2では、上記実施の形態1のように構造体生成/破棄処理（図5）および構造体破棄処理（図6）を並列に行うのではなく、1つの構造体生成/破棄処理として実行するものである。なお、本実施の形態2においても、構造体数検出処

10

20

30

40

50

理は、当該構造体生成／破棄処理と並列に行われる。

【0049】侵入検出部11は、通信路12からパケットを取得すると（ステップV1）、当該パケットのヘッダを抽出し（ステップV2）、当該ヘッダ中のセッション識別子に基づいて構造体生成処理を実行する（ステップV3～V5）。

【0050】より具体的には、侵入検出部11は、当該セッション識別子に対応する構造体が存在するか否かを判別する（ステップV3）。当該セッション識別子に対応する構造体が存在していれば（ステップV3のYES）、侵入検出部11は、セッション拡張情報の最終パケット到着時刻および総パケット数を更新するとともに、取得されたパケット自体を含む到着パケット情報を新たに生成し、当該到着パケット情報を構造体に追加する（ステップV4）。

【0051】一方、上記セッション識別子に対応する構造体が存在していなければ（ステップV3のNO）、侵入検出部11は、当該セッション識別子に対応する構造体を新たに生成する（ステップV5）。この場合、侵入検出部11は、セッション基本情報、セッション拡張および到着パケット情報を構造体として生成する。

【0052】さらに、侵入検出部11は、取得されたパケットのヘッダを参照し、当該パケットが最終パケットであるか否かを判別する（ステップV6）。最終パケットでなければ（ステップV6のNO）、侵入検出部11は、次に、既に取得され到着パケット情報として保持されているパケットの中に最終パケットがあるか否かを判別する（ステップV7）。パケットの送信経路によっては最終パケットが途中のパケットよりも先に到着することがあるからである。

【0053】到着パケット情報の中にも最終パケットがなければ（ステップV7のNO）、侵入検出部11は、当該処理を終了する。一方、到着パケット情報の中に最終パケットがあれば（ステップV7のYES）、侵入検出部11は、一連のパケットをすべて取得したか否かを判別する（ステップV8）。また、ステップV6の結果、取得されたパケットが最終パケットであると判別された場合にも、当該ステップV8に係る一連のパケットをすべて取得したか否かの判別処理を実行する。

【0054】当該判別処理は、取得された最終パケットまたは到着パケット情報として保持されている最終パケットのヘッダに記述されている総パケット数とセッション拡張情報中の総パケット数とを比較し、一致しているか否かを判別する処理である。一致していなければ（ステップV8のNO）、途中のパケットの到着が遅れていると考えられるから、侵入検出部11は、当該処理を終了する。一致していれば（ステップV8のYES）、一連のパケットがすべて取得されたと考えられるから、侵入検出部11は、パケット結合処理を実行する（ステップV9～V13）。すなわち、一連のパケットをすべて取

得した後からパケット結合処理を実行する。

【0055】より具体的には、侵入検出部11は、各到着パケット情報のヘッダ中のシーケンス番号を参照し、先頭のシーケンス番号に係るパケットから順次累積的に結合していく。さらに具体的には、侵入検出部11は、対象パケットと次パケットとを正常に結合できるか否かを判別する（ステップV9）。さらに具体的には、侵入検出部11は、最初に先頭パケットを対象とし、当該先頭パケットのヘッダ中の次パケットのパケット長とシーケンス番号から見た場合における2番目のパケットのパケット長とが一致するか否かを判別する。一致していれば（ステップV9のYES）、侵入検出部11は、2番目のパケットを先頭パケットに結合する（ステップV10）。

【0056】その後、侵入検出部11は、すべてのパケットの結合が終了したか否かを判別する（ステップV11）。この場合、すべてのパケットの結合が終了していないので、侵入検出部11は、2番目のパケットを対象とし、上記ステップV9の判別処理に移行する。パケットを正常に結合することができ、その結果すべてのパケットの結合が終了すれば（ステップV11のYES）、当該セッションは正常セッションであると考えられ、かつ正常アクセスであると考えられるから、侵入検出部11は、当該構造体を破棄する（ステップV12）。

【0057】一方、ステップV9の結果、次パケット長と次パケットの実際のパケット長とが一致していなければ、不正パケットである可能性が極めて高いため、侵入検出部11は、この時点で以後のパケットの結合処理を中止し、当該構造体の保留を決定する（ステップV13）。

【0058】図10は、ルータ2の構成を機能的に説明するための概念図である。ルータ2は、通信プロトコルの階層として、物理層、データリンク（D/L）層、IP層、TCP層および上位AP層を有している。また、ルータ2は、ネットワーク層であるIP層およびトランスポート層であるTCP層の間にIDS層を有している。ルータ2に到達するパケットは、IP層およびTCP層を介してIDS層において処理され、ヘッダからデータまでを関連付けて監視される。すなわち、ネットワーク層よりも上位層でパケットが管理される。

【0059】以上のようにこの実施の形態2によれば、一連のパケットを正常に組み立てることができるか否かに基づいて構造体を保留するか否かを決定している。したがって、不正パケットのセッション識別子はパケットごとと異なるために本来ならば構造体が急激に増加するはずであるのに、セッション識別子が不正に書き換えられて1つのデータ構造体しか生成されないような場合でも、その構造体が不正アクセスに対応しているものであることを検出できる。そのため、不正アクセスの侵入を精度良く検出できるので、DDoS攻撃などを精度良くかつ

自動的に検出できる。よって、セキュリティ信頼性のあるシステム構築を実現することができる。

【0060】実施の形態3

上記実施の形態2では、一連のバケットをすべて取得した後バケット結合処理を実行している。これに対して、本実施の形態3では、一連のバケットを取得している途中においてバケット結合処理を実行している。これにより、構造体の保留/破棄を迅速に決定でき、その結果DDoS攻撃などを迅速に検出することができる。

【0061】上述のように、不正バケットにおいてはヘッダと実際のバケットとの間の整合性はないので、一連のバケットを取得している最中においても結合処理を行えば不正バケットであるか否かを判断することができる。そこで、本実施の形態3では、バケットが取得されるたびにバケットの結合処理を実行し、正常に結合できなかった時点においてその構造体を保留すると決定するようにしている。

【0062】図11は、本実施の形態3に係る構造体生成/破棄処理を説明するためのフローチャートである。本実施の形態3においても、上記実施の形態2と同様に、構造体生成/破棄処理および構造体破棄処理を1つの処理として実行し、かつ、当該構造体生成/破棄処理と並列に、構造体数検査処理を実行する。

【0063】侵入検出部11は、通信路12からバケットを取得すると（ステップW1）、上述と同様に、当該バケットからヘッダを抽出し（ステップW2）、当該ヘッダ中のセッション識別子に対応する構造体が存在するか否かを判別する（ステップW3）。構造体があれば（ステップW3のYES）、侵入検出部11は、当該構造体を更新する（ステップW4）。一方、構造体が無ければ（ステップW3のNO）、侵入検出部11は、上記セッション識別子に対応する構造体を新たに生成する（ステップW5）。

【0064】また、侵入検出部11は、既存の構造体を更新する際に、新たに取得されたバケットと取得済のバケットとの結合を試みる。より具体的には、侵入検出部11は、取得されたバケットおよび既に保持されているバケットのヘッダに記述されているシーケンス番号に基づいて、取得されたバケットの前バケットまたは次バケットを検索し、いずれかに連続するバケットが保持されているか否かを判別する（ステップW6）。さらに具体的には、侵入検出部11は、取得されたバケットのヘッダに記述されているシーケンス番号と保持されている1または複数のバケットのヘッダに記述されているシーケンス番号とを比較することにより、前バケットまたは次バケットを検索する。

【0065】その結果、シーケンス番号から見て連続するバケットが保持されている場合（ステップW6のYES）、侵入検出部11は、取得されたバケットと当該連続するバケットとを結合できるか否かを判別する（ステ

ップW7）。より具体的には、取得されたバケットの次バケットが保持されている場合、侵入検出部11は、保持されている次バケットのバケット長が取得されたバケットのヘッダに記述されている次バケット長と一致するか否かを判別する。また、取得されたバケットの前バケットが保持されている場合、侵入検出部11は、取得されたバケットのバケット長が保持されている前バケットのヘッダに記述されている次バケット長と一致するか否かを判別する。すなわち、連続するバケット間で整合性がとれているか否かに基づいて、結合可能であるか否かを判別することとしている。

【0066】ヘッダに記述されている情報と整合性がとれていて結合可能である場合（ステップW7のYES）、侵入検出部11は、取得されたバケットと保持されているバケットとを結合する（ステップW8）。一方、シーケンス番号では確かに連続するバケットであるけれども次バケット長などのヘッダの情報から整合性がなく結合不能である場合（ステップW7のNO）、侵入検出部11は、この時点において当該構造体を保留することを決定する（ステップW9）。

【0067】上記ステップW8においてバケットを結合した後、侵入検出部11は、すべてのバケットの結合が完了したか否かを判別する（ステップW10）。まだ完了していなければ（ステップW10のNO）、侵入検出部11は、当該処理を終了する。一方、完了すれば（ステップW10のYES）、当該アクセスは正常アクセスである可能性が極めて高いため、侵入検出部11は、当該構造体を破棄する（ステップW11）。

【0068】以上のように本実施の形態3によれば、一連のバケットを取得している最中においてバケット結合処理を実行し、正常に組み立てることができない場合に、その時点において構造体の保留を決定する。したがって、構造体の保留/破棄を迅速に決定することができる。そのため、構造体の総数を検査する周期を短くしても、単なるアクセス量の増大を不正アクセスであると誤検出することがない。よって、不正アクセス検出に要する時間を短縮することができ、被害拡大を迅速に防ぐことができる。

【0069】実施の形態4

図12は、本発明の実施の形態4に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。図12において、図1と同じ機能部分については同一の参照符号を使用する。

【0070】上記実施の形態1ないし3では、1つの内部ネットワーク3が1つのルータ2を介して外部ネットワーク1に接続されている構成を例にとっている。これに対して、本実施の形態4では、複数の内部ネットワーク20A、20Bを有し、当該複数の内部ネットワーク20A、20Bと外部ネットワーク1とをそれぞれルータ21A、21Bを介して接続した構成を例にとっている。

10

20

30

40

50

る。

【0071】より具体的には、このコンピュータシステムは、2つの内部ネットワーク20A、20Bを有し、いずれもルータ21A、21Bを介して外部ネットワーク1に接続されている。各内部ネットワーク20A、20B同士もまた、ルータ22を介して接続されている。2つの内部ネットワーク20A、20Bは、たとえば同じ企業の異なる部署内に構築されている。すなわち、本実施の形態4では、不正アクセスを同時期に受ける可能性のある2つの内部ネットワーク20A、20Bを有するコンピュータネットワークを前提にしている。さらに、このコンピュータネットワークは、上位管理装置23を備えている。上位管理装置23は、内部ネットワークに関連して設けられ、2つのルータ21A、21Bに専用線24A、24Bを介して接続されている。

【0072】図13は、上記2つのルータ21A、21Bおよび上位管理装置23の内部構成を示すブロック図である。2つのルータ21A、21Bは、いずれも、実施の形態1ないし3と同様に、ルーティング部10および侵入検出部11を有している。このうち侵入検出部11は、実施の形態1ないし3のいずれかと同様に、セッションごとに構造体を生成して一定期間ごとにその数を検証することにより不正アクセスの検出を行っている。また、各ルータ21A、21Bは、不正アクセスの侵入を検出した場合に、不正アクセス検出信号を専用線24A、24Bを介して上位管理装置23に送信する。不正アクセス検出信号は、不正アクセスを検出したことを示すデータを含むものである。

【0073】上位管理装置23は、侵害判定部23aを有している。侵害判定部23aは、2つのルータ21A、21Bから不正アクセス検出信号を受信したか否かに基づいて、不正アクセスの侵入の有無を判定するものである。上述のように、2つのルータ21A、21Bは、不正アクセスを同時期に受ける可能性のあるものである。したがって、一方のルータで不正アクセスが検出された場合、他方のルータでも不正アクセスが検出される可能性がある。しかし、一方のルータにおいて不正アクセスであると検出された場合であっても、他方のルータにおいてあまり構造体数が多くなければ、単なるアクセス量増加の可能性もある。そのため、上位管理装置23において、両方のルータ21A、21Bから不正アクセス検出信号を受信したことを条件として、不正アクセスの侵入があると判定することとしている。判定結果は、不正アクセス検出信号の送信元のルータ、または両方のルータに送信される。

【0074】図14は、侵入検出部11において実行される構造体数検査処理を説明するためのフローチャートである。上述のように、侵入検出部11は、検出周期の開始にตอบสนองして（ステップX1のYES）、保持している構造体の総数nが不正検出しきい値nth以上であるか

否かを判別する（ステップX2）。構造体の総数nが不正検出しきい値nth未満であれば（ステップX2のNO）、侵入検出部11は、当該処理を終了する。一方、構造体の総数nが不正検出しきい値nth以上であれば（ステップX2のYES）、侵入検出部11は、ポート遮断をルーティング部10に通知するのに先立って、不正アクセス検出信号を作成し、当該不正アクセス検出信号を専用線24Aまたは24Bを介して上位管理装置23に送信する（ステップX3）。

【0075】上位管理装置23は、後述するように、他方のルータから不正アクセス検出信号を受信したか否かに応じて判定信号をルータに送信する。そこで、侵入検出部11は、不正アクセス検出信号を上位管理装置23に送信した後、判定信号を受信したか否かを判別する（ステップX4）。

【0076】判定信号を受信した場合、当該判定信号が肯定を示していれば、確かに不正アクセスが発生していると考えられるから、侵入検出部11は、ルーティング部10にアクセスし、外部ネットワーク1との接続ポートを遮断させる（ステップX5）。一方、判定信号を受信した場合に当該判定信号が否定を示していれば、単なるアクセス量の増加であると考えられるから、侵入検出部11は、当該処理を終了する。

【0077】図15は、上位管理装置23の侵害判定部23aにおける侵害判定処理を説明するためのフローチャートである。侵害判定部23aは、不正アクセス検出信号を受信したか否かを判別する（ステップY1）。不正アクセス検出信号を受信すると（ステップY1のYES）、侵害判定部23aは、他方のルータから不正アクセス検出信号を受信したか否かを判別する（ステップY2）。侵害判定部23aは、当該判別処理の開始から予め定められた一定時間が経過したか否かを判別し（ステップY3）、上記一定時間が経過するまで上記判別処理を繰り返し実行する。2つのルータから不正アクセス検出信号が送信されるのにはある程度の時間差があることが予想され、上記一定時間は上記時間差を考慮して設定されている。

【0078】上記ステップY3において一定時間が経過したと判別されるまでの間に、上記ステップY2において他方のルータから不正アクセス検出信号を受信したと判別されると、侵害判定部23aは、不正アクセスの発生を肯定する判定信号を両方のルータに送信する（ステップY4）。一方、上記ステップY2において他方のルータから不正アクセス検出信号を受信したと判別されないまま上記一定時間が経過した場合、不正アクセス検出信号の送信元であるルータへの単なるアクセス量の増加であると考えられるから、侵害判定部23aは、不正アクセスの発生を否定する判定信号を上記送信元のルータに送信する（ステップY5）。

【0079】図16は、上述のルータ21A、21Bの

構成を機能的に説明するための概念図である。ルータ21A、21Bは、いずれも、通信プロトコルの階層として、物理層、データリンク(D/L)層、IP層、TCP層および上位AP層を有している。ルータ21は、パケットをネットワーク層であるIP層あるいはトランスポート層であるTCP層で管理している。IP層またはTCP層での管理結果は、上位管理装置23に通知される。

【0080】以上のようにこの実施の形態4によれば、複数のルータにて不正アクセスの侵入が検出された場合に、それらの検出結果を一元的に集めることにより、不正アクセスの侵入があるか否かを判定している。したがって、1つのルータにおいて不正アクセスを検出するよりも、不正アクセスを受けていることを高精度に判断することができる。そのため、セキュリティの信頼性をより一層高めることができる。

【0081】なお、上述の説明では、2つの内部ネットワーク20A、20Bがそれぞれルータ21A、21Bを介して外部ネットワーク1に接続されている構成を例にとっている。しかし、3以上の内部ネットワーク3をそれぞれルータを介して外部ネットワーク1に接続しているコンピュータネットワークにおいても、当該実施の形態4と同様の構成を採用することができる。

【0082】実施の形態5

上記実施の形態4では、上位管理装置23において複数のルータ21A、21Bへのアクセス状況を監視し、上位管理装置23において不正アクセス検出の最終判断を行っており、ルータ21A、21Bは単に上位管理装置23の判断に従うのみである。これに対して、本実施の形態5では、1つのルータにおいて不正アクセスの侵入が検出された場合、当該ルータが他のルータのアクセス状況を参照することにより、不正アクセスであるか否かの最終判断をルータ自身において行うこととしている。

【0083】より詳述すれば、本実施の形態5に係るコンピュータシステムは、上記実施の形態4と同様に、2つの内部ネットワーク20A、20Bをそれぞれルータ21A、21Bを介して外部ネットワーク1に接続した構成となっており、内部ネットワーク20A、20Bに関連して各ルータ21A、21Bに接続された上位管理装置23を備えている。当該コンピュータシステムは、さらに、図12に破線で示すように、ルータ21A、21B同士を専用線30を介して相互接続している。より具体的には、当該コンピュータシステムは、図13に破線で示すように、各ルータ21A、21B内の侵入検出部11同士を専用線30を介して相互接続している。

【0084】図17は、本実施の形態5に係る構造体数検査処理を説明するためのフローチャートである。侵入検出部11は、上述のように、侵入検出部11は、検出周期の開始にตอบสนองして(ステップZ1のYES)、保持している構造体の総数nが不正検出しきい値nth以上で

あるか否かを判別する(ステップZ2)。構造体の総数nが不正検出しきい値nth未満であれば(ステップZ2のNO)、侵入検出部11は、当該処理を終了する。一方、構造体の総数nが不正検出しきい値nth以上であれば(ステップZ2のYES)、侵入検出部11は、ポート遮断をルーチング部10に通知するのに先立って、アクセス状況確認信号を作成し、当該アクセス状況確認信号を専用線を介して他のルータに送信する(ステップZ3)。上記アクセス状況確認信号は、他のルータのアクセス状況を確認するためのものである。より具体的には、上記アクセス状況確認信号は、他のルータのアクセス状況の返信を指示するメッセージを含むものである。

【0085】他のルータは、後述するように、自ルータのアクセス状況、具体的には構造体の総数nを含む返信信号を送信元のルータに返信する。そこで、侵入検出部11は、返信信号を受信したか否かを判別する(ステップZ4)。返信信号を受信した場合(ステップZ4のYES)、侵入検出部11は、当該返信信号に含まれている構造体の総数nに基づいて、他のルータのアクセス状況を確認する(ステップZ5)。

【0086】より具体的には、侵入検出部11は、上記返信信号に含まれている構造体の総数nが上記不正検出しきい値nthよりも小さな第2のしきい値kth以上であるか否かを判別する。上記第2のしきい値kthは、これ以上構造体があれば不正アクセスである蓋然性が高いと考えられる値に設定されている。たとえば、第2のしきい値kthは、不正検出しきい値nthよりも数10%ほど小さな値である。

【0087】上記構造体の総数nが第2のしきい値kth未満であれば、自ルータに対してのみアクセス量が増加していると考えられるから、侵入検出部22は、当該処理を終了する。一方、上記構造体の総数nが第2のしきい値kth以上であれば、他のルータにおいてもアクセス量が非常に多く不正アクセスである蓋然性が非常に高いと考えられるから、侵入検出部11は、ルーチング部10にアクセスして外部ネットワーク1との接続ポートの遮断を指示する(ステップZ6)。また、侵入検出部11は、不正アクセスの侵入を検出した旨のメッセージを含む報告信号を上位管理装置23に送信する(ステップZ7)。

【0088】図18は、本実施の形態5に係る侵入検出部11におけるアクセス状況返信処理を説明するためのフローチャートである。このアクセス状況返信処理は、上記構造体数検査処理と並列に行われるものである。

【0089】侵入検出部11は、他のルータからアクセス状況確認信号を受信したか否かを判別する(ステップR1)。アクセス状況確認信号を受信した場合、侵入検出部11は、アクセス状況を送信元のルータに通知する(ステップR2)。より具体的には、アクセス状況を含む返信信号を送信元のルータに送信する。さらに具体的

には、構造体記憶部11bに記憶されている構造体の総数nを含む返信信号を作成し、当該返信信号を送信元のルータに送信する。

【0090】図19は、上述のルータ21A、21Bの構成を機能的に説明するための概念図である。ルータ21A、21Bは、いずれも、通信プロトコルの階層として、物理層、データリンク(D/L)層、IP層、TCP層および上位AP層を有している。ルータ21のTCP層は、不正アクセスの侵入の有無を検出する。ルータ21のTCP層は、その検出結果を他方のルータ21のTCP層に通知し、他方のルータ21のTCP層からアクセス状況の通知を受ける。また、ルータ21のTCP層は、当該アクセス状況を上位管理装置に通知する。

【0091】以上のように本実施の形態5によれば、他のルータのアクセス状況を確認することにより、ルータ内の侵入検出部自身において不正アクセスの侵入の有無を判別している。したがって、上位管理装置23にて両方の不正アクセス検出信号を待って不正アクセスであるか否かを判定するよりも、不正アクセスであることを迅速に判断することができる。そのため、不正アクセスに対する措置を迅速にとることができる。

【0092】なお、上述の説明では、2つの内部ネットワーク20A、20Bがそれぞれルータ21A、21Bを介して外部ネットワーク1に接続されている構成を例にとっている。しかし、3以上の内部ネットワーク3をそれぞれルータを介して外部ネットワーク1に接続しているコンピュータネットワークにおいても、当該実施の形態5と同様の構成を採用することができる。

【0093】実施の形態6

図20は、本発明の実施の形態6に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。図20において、図1と同じ機能部分については同一の参照符号を使用する。

【0094】上記実施の形態5では、自ルータのアクセス量の増加が不正アクセスであるか否かを確認するために、他のルータのアクセス状況を参照している。これに対して、本実施の形態6では、自ルータのアクセス量の増加が不正アクセスであるか否かを確認するために他のルータのアクセス状況を参照するとともに、他のルータの不正検出しきい値n_{th}を他のルータ自身で補正することとしている。

【0095】より詳述すれば、複数のルータは、上述のように、各々同一の不正検出しきい値n_{th}を使用して不正アクセス検出を行っている。一方、複数のルータは不正アクセスを同時に受ける可能性のあるもの同士であるので、1つのルータにおいて不正アクセスが検出されれば、他のルータにおいても不正アクセスを受けている可能性がある。しかし、構造体の数が不正検出しきい値n_{th}以上となるタイミングはルータによってばらつく場合が多く、しかもそのタイミングのばらつきは以後の不正

アクセスにおいても同様の傾向を示すものと考えられる。そこで、本実施の形態7では、不正アクセス検出のタイミングのずれを考慮し、不正検出しきい値n_{th}をルータ単位で動的に補正することにより、不正アクセスの検出速度を向上させ、被害拡大を迅速に阻止し得るようにしている。

【0096】本実施の形態6に係るコンピュータネットワークは、複数の内部ネットワーク40A、40B、40C、40Dを有し、各々ルータ41A、41B、41C、41D（以下総称するときは「ルータ41」という）を介して外部ネットワーク1に接続されている。これら各ルータ41A、41B、41C、41Dは、論理的に隣接するルータと専用線42を介して接続されている。より具体的には、複数のルータ41A～41Dは、専用線42を介して環状に接続されている。また、このコンピュータネットワークは、複数の内部ネットワーク40A～40Dに関連して設けられた上位管理装置43を備えている。上位管理装置43は、各ルータ41A、41B、41C、41Dに専用線44A、44B、44C、44Dを介してそれぞれ接続され、すべてのルータ41A～41Dにおけるアクセス状況を監視する機能を有している。なお、内部ネットワーク40同士もルータ46を介してそれぞれ相互接続されている。

【0097】図21は、複数のルータ41の内部構成を示すブロック図である。各ルータ41は、上記実施の形態1ないし5と同様に、それぞれ、侵入検出部11およびルーチング部10を備えている。各侵入検出部11は、論理的に隣接するルータ41の侵入検出部11と専用線42を介して相互接続されている。また、各侵入検出部11は、複数の補正しきい値m_{th}を記憶する補正しきい値記憶部50を有している。上記補正しきい値m_{th}は、少なくとも不正検出しきい値n_{th}よりも小さな値で、アクセス量が急激に増加したときに不正検出しきい値n_{th}の補正值として利用されるものである。補正しきい値m_{th}は、たとえば、不正検出しきい値n_{th}よりも数%ずつ小さくなる複数の値である。なお、補正しきい値m_{th}を1つだけ設定してもよいことはもちろんである。

【0098】図22は、侵入検出部11における構造体数検査処理を説明するためのフローチャートである。侵入検出部11は、検出周期の開始に反応して（ステップN1のYES）、構造体記憶部11bに保有している構造体の総数nがしきい値記憶部11aに記憶されている不正検出しきい値n_{th}以上であるか否かを判別する（ステップN2）。構造体の総数nが不正検出しきい値n_{th}未満であれば（ステップN2のNO）、侵入検出部11は、当該処理を終了する。一方、構造体の総数nが不正検出しきい値n_{th}以上であれば（ステップN2のYES）、侵入検出部11は、ポート遮断をルーチング部10に通知するのに先立って、補正指示信号を作成し、当該補正指示信号を専用線42を介して隣接するルータ4

1に送信する(ステップN3)。上記補正指示信号は、上記構造体の総数nと不正検出しきい値n_{th}の補正を指示する旨のメッセージとを含むものである。

【0099】1つのルータの侵入検出部から補正指示信号が送信されると、他のすべてのルータの侵入検出部は、各々のアクセス状況、具体的には構造体の総数nおよび補正の有無結果を含む返信信号を送信元のルータに返信する。そこで、侵入検出部11は、補正指示信号を送信した後、他のすべての関連するルータから返信信号を受信したか否かを判別する(ステップN4)。

【0100】すべての返信信号を受信すると(ステップN4のYES)、侵入検出部11は、当該返信信号に含まれているアクセス状況に基づいて、自ルータのアクセス量増加は不正アクセスであるか否かを判別する(ステップN5)。より具体的には、侵入検出部11は、構造体の総数nが第2のしきい値k_{th}以上であるか否かをすべての返信信号について判別する。また、侵入検出部11は、当該判別結果に基づいて、構造体の総数nが第2のしきい値k_{th}以上である割合が一定割合以上であるか否かを判別する。

【0101】一定割合以上であれば、他のルータでもアクセス量が急激に増加して不正アクセスである蓋然性が高いと考えられるから、侵入検出部11は、ルーティング部10に対して接続ポートを遮断させる(ステップN6)。その後、ステップN7に移行する。一方、一定割合未満であれば、単なるアクセス量の増加と考えられるから、侵入検出部11は、ステップN7に直接移行する。

【0102】ステップN7は、関連するすべてのルータ41における補正状況を上位管理装置に通知する処理である。より具体的には、侵入検出部11は、返信信号に含まれている補正の有無結果を上位管理装置43に送信する。これにより、上位管理装置43は、関連するすべてのルータ41の不正検出しきい値n_{th}の状況を一元管理することができる。

【0103】図23は、侵入検出部11のアクセス状況返信処理を説明するためのフローチャートである。侵入検出部11は、補正指示信号を受信すると(ステップM1)、不正検出しきい値n_{th}の補正の必要性を判断する(ステップM2)。より具体的には、侵入検出部11は、構造体記憶部11bに記憶されている構造体の総数nと補正しきい値記憶部50に記憶されている補正しきい値m_{th}とを比較し、構造体の総数nがすべての補正しきい値m_{th}以上であるか否かを判別する。

【0104】構造体の総数nよりも大きな補正しきい値m_{th}がある場合(ステップM2のNO)、補正の必要があるから、侵入検出部11は、現在の不正検出しきい値n_{th}を補正する(ステップM3)。より具体的には、侵入検出部11は、複数の補正しきい値m_{th}のうち現在の不正検出しきい値n_{th}よりも小さく、かつその中で最も

大きな補正しきい値m_{th}を特定する。侵入検出部11は、この特定された補正しきい値m_{th}を新たな不正検出しきい値n_{th}として設定する。その後、侵入検出部11は、アクセス状況、具体的には上記構造体の総数nと補正有のメッセージとを含む返信信号を作成し、当該返信信号を送信元のルータ41に返信する(ステップM4)。

【0105】一方、構造体の総数nがすべての補正しきい値m_{th}以上である場合(ステップM2のYES)、補正の必要はないから、侵入検出部11は、不正検出しきい値n_{th}を補正することなく、アクセス状況、具体的には構造体の総数nと補正無のメッセージとを含む返信信号を作成し、当該返信信号を送信元のルータ41に返信する(ステップM5)。

【0106】さらに、侵入検出部11は、上記受信された補正指示信号を論理的に隣接する2つのルータのうち、補正指示信号を送信してきたルータとは別のルータに対して、上記補正指示信号を転送する(ステップM6)。

【0107】図24は、上述の4つのルータのうちルータ41A、41B、41Cの構成を機能的に説明するための概念図である。ルータ41は、通信プロトコルの階層として、物理層、データリンク(D/L)層、IP層、TCP層および上位AP層を有している。

【0108】たとえばルータ41AのTCP層において不正アクセスが検出された場合、当該ルータ41Aの上位AP層は、不正アクセスを検出したことおよび構造体の総数nを隣接するルータ41Bの上位AP層に通知する。ルータ41Bの上位AP層は、当該通知に回答して不正検出しきい値n_{th}を補正しあるいは補正することなく、アクセス状況および補正の有無を送信元のルータ41Aの上位AP層に返信する。また、ルータ41Bの上位AP層は、ルータ41Aからの通知を隣接するルータ41Cの上位AP層に通知する。ルータ41Cの上位AP層は、上記通知に回答して不正検出しきい値n_{th}を補正しあるいは補正することなく、アクセス状況および補正の有無をルータ41Bの上位AP層に返信する。ルータ41Bの上位AP層は、当該返信内容をさらにルータ41Aに返信する。さらに、ルータ41Aの上位AP層は、これら関連するすべてのルータのアクセス状況および/または補正の有無を上位管理装置43に通知する。

【0109】以上のように本実施の形態6によれば、他のルータのアクセス状況を参照することにより、アクセス量の増加が不正アクセスであるか否かを判別している。したがって、不正アクセスの検出精度を向上できる。しかも、他のルータにおいて不正検出しきい値n_{th}をアクセス状況に応じて補正しているから、もしもその後不正アクセスがあった場合でもそれを迅速に検出することができる。そのため、被害拡大を最小限に抑えることができる。

【0110】実施の形態7

図25は、本発明の実施の形態7に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。図25において、図1と同じ機能部分については同一の参照符号を使用する。

【0111】上記実施の形態1ないし6では、ルータは到達するすべてのパケットを不正アクセス検出の対象としている。これに対して、本実施の形態7では、1つの内部ネットワークに対して複数のルータを接続し、各ルータを1つのサービス種別にそれぞれ対応付けるとともに、各ルータにおいて対応するサービス種別のパケットのみを不正アクセス検出の対象としている。ただし、対応するサービス種別以外のパケットを無条件に内部ネットワークに進入させるのではなく、そのようなパケットについては別のサーバ（おとりサーバ）に転送し、当該おとりサーバにおいて不正パケットであるか否かを監視することとしている。

【0112】複数のサービスを提供する1つの内部ネットワークがある場合、1つのルータですべてのサービス種別のパケットを不正アクセス検出の対象とすると、当該ルータの負荷が大きく、不正パケットであってもそれを看過するおそれがある。そこで、ルータの負荷を軽減すべく、上記内部ネットワークに対して複数のルータを接続するとともに、1つのルータにおいては1つのサービス種別のパケットのみを不正アクセスの検出対象とすることとしている。ただし、上述したように、1つのルータに到達した他のサービス種別のパケットを無条件に通過させるのは危険であるため、各ルータにそれぞれ対応するおとりサーバを設け、当該おとりサーバにて不正アクセスの検出を行うこととしている。

【0113】より詳述すれば、1つの内部ネットワーク3は、複数のルータ60A、60B、60C（以下総称するときは「ルータ60」という）を介して外部ネットワーク1に接続されている。各ルータ60A、60B、60Cは、それぞれ、1つのサービス種別に対応している。本実施の形態7に係る内部ネットワーク1が提供するサービス種別は、たとえば、メールサービス、ウェブサービスおよびFTPサービスである。これらのサービス種別は、パケットのヘッダに記述されている送信先ポートにより識別可能である。

【0114】各ルータ60A、60B、60Cには、それぞれ、おとりサーバ61A、61B、61C（以下総称するときは「おとりサーバ61」という）が接続されている。各おとりサーバ61A、61B、61Cは、それぞれ、内部ネットワーク3にて提供される複数のサービス種別のうち、接続されているルータ60A、60B、60Cに対応付けられているサービス種別以外のサービス種別のパケットを対象とし、不正アクセスの侵入の有無を検出する。おとりサーバ61には、ルータ60にてコピーされたパケットが与えられるようになってい

る。

【0115】図26は、本実施の形態7に係る侵入検出部11における構造体生成／破棄処理を説明するためのフローチャートである。なお、本実施の形態7においては、当該構造体生成／破棄処理と並列に、たとえば図7に示された構造体数検査処理が行われる。

【0116】侵入検出部11は、通信路12からパケットを取得すると（ステップQ1）、当該パケットのヘッダを抽出する（ステップQ2）。その後、侵入検出部11は、当該抽出されたヘッダ中の送信ポートを参照し、対象パケットであるか否かを判別する（ステップQ3）。すなわち、対象とするサービス種別に対応するパケットであるか否かを判別する。

【0117】対象パケットであれば（ステップQ3のYES）、侵入検出部11は、上記実施の形態1ないし3のいずれかで説明した構造体の生成／更新および破棄に関する処理を実行する（ステップQ4）。具体的には、侵入検出部11は、実施の形態1で説明した図5におけるステップS3～S9の処理を実行する。または、侵入検出部11は、実施の形態2で説明した図9におけるステップV3～V13の処理を実行する。または、侵入検出部11は、実施の形態3で説明した図11におけるステップW3～W11の処理を実行する。

【0118】一方、対象パケットでなければ（ステップQ3のNO）、侵入検出部11は、当該パケットの検査を禁止する（ステップQ5）。すなわち、当該パケットについて構造体の生成／更新処理を行わない。しかし、何らの検査もしなければ不正アクセスを看過するかもしれないから、侵入検出部11は、当該パケットをコピーし（ステップQ6）、当該コピーされたパケットを対応するおとりサーバ61に転送する（ステップQ7）。

【0119】図27は、本実施の形態7に係るおとりサーバ61における構造体生成／破棄処理を説明するためのフローチャートである。このおとりサーバ61においても、当該構造体生成／破棄処理と並列に、たとえば図7に示された構造体数検査処理を実行する。

【0120】おとりサーバ61は、ルータ60の侵入検出部11からパケットを受信すると（ステップP1のYES）、上記実施の形態1ないし3のいずれかで説明したパケットに対応する構造体の生成／更新および破棄に関する処理を実行する（ステップP2）。具体的には、侵入検出部11は、実施の形態1で説明した図5におけるステップS3～S9の処理を実行する。または、侵入検出部11は、実施の形態2で説明した図9におけるステップV3～V13の処理を実行する。または、侵入検出部11は、実施の形態3で説明した図11におけるステップW3～W11の処理を実行する。

【0121】これにより、対応するルータ60において対象とするサービス種別以外のパケットの検査を実行することができる。したがって、おとりサーバ61におい

て攻撃ログを収集することができる。そのため、不正者探知への応用も可能となる。

【0122】図28は、ルータ60の構成を機能的に説明するための概念図である。ルータ60は、通信プロトコルの階層として、物理層、データリンク(D/L)層、IP層、TCP層および上位AP層を有している。また、ルータ60は、ネットワーク層であるIP層およびトランスポート層であるTCP層の間にIDS層を有している。

【0123】ルータ2に到達するパケットのうち対象とするサービス種別のパケットは、IP層およびTCP層を介してIDS層において処理され、ヘッダからデータまでを関連付けて監視される。すなわち、ネットワーク層よりも上位層でパケットが管理される。また、対象とするサービス種別以外のパケットは、IP層からおとりサーバ61に誘導され、当該おとりサーバ61にて検査される。

【0124】以上のようにこの実施の形態7によれば、1つのルータ60に対して不正アクセス検出の対象パケットを1つのサービス種別に絞り込んでいるので、すべてのサービス種別のパケットを不正アクセス検出の対象とする場合に比べて、ルータの負荷を大幅に軽減できる。したがって、不正アクセスの検出精度を向上できる。そのため、セキュリティ精度の向上を一層図ることができる。

【0125】しかも、対象のサービス種別以外のパケットについては、コピーをしておとりサーバ61に転送し、当該おとりサーバ61にて不正アクセスの検出対象としている。したがって、サービス種別以外の不正パケットについても検出することができる。そのため、1つのサービス種別につき不正アクセス検出の確実性を向上できるから、全体として、不正アクセス検出の精度を向上できる。よって、セキュリティ精度の向上を図ることができる。

【0126】なお、上述の説明では、1つの内部ネットワーク3が複数のサービスを提供する場合を例にとって説明している。しかし、たとえば内部ネットワーク3が1つのサービスのみを提供する場合には、内部ネットワーク3を1つのルータを介して外部ネットワーク1に接続し、当該ルータを上記1つのサービス種別に対応付けるようにすればよい。

【0127】他の実施の形態本発明の実施の形態の説明は以上のとおりであるが、本発明は上述の実施の形態以外にも適用可能である。たとえば上記すべての実施の形態においては、EtherIIフレームだけでなく、Ethernet802.3フレーム、Ethernet802.2フレーム、EthernetSNAPなどすべてのEtherフレームを用いることができる。

【0128】

【発明の効果】以上のように本発明によれば、パケットのヘッダに記述されているネットワーク層およびトラン

スポート層のデータに基づいてセッションごとに対応する構造体を生成し、当該構造体が異常な数になった場合に不正アクセスの侵入を検出する。したがって、大量の異なるセッションを確立するDDoS攻撃などの不正アクセスの侵入を精度良く検出できる。また、過去ログを解析することなく不正アクセスの侵入を自動的に検出できる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。

【図2】 パケットの構成を示す概念図である。

【図3】 ルータの内部構成を示すブロック図である。

【図4】 構造体を示す概念図である。

【図5】 構造体生成/破棄処理を説明するためのフローチャートである。

【図6】 構造体破棄処理を説明するためのフローチャートである。

【図7】 構造体数検査処理を説明するためのフローチャートである。

【図8】 本実施の形態2に係る構造体を示す概念図である。

【図9】 本実施の形態2に係る構造体生成/破棄処理である。

【図10】 ルータの構成を機能的に説明するための概念図である。

【図11】 本実施の形態3に係る構造体生成/破棄処理を説明するためのフローチャートである。

【図12】 本発明の実施の形態4に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。

【図13】 2つのルータおよび上位管理装置の内部構成を示すブロック図である。

【図14】 侵入検出部において実行される構造体数検査処理を説明するためのフローチャートである。

【図15】 上位管理装置の侵害判定部における侵害判定処理を説明するためのフローチャートである。

【図16】 上述のルータの構成を機能的に説明するための概念図である。

【図17】 本実施の形態5に係る構造体数検査処理を説明するためのフローチャートである。

【図18】 本実施の形態5に係る侵入検出部におけるアクセス状況返信処理を説明するためのフローチャートである。

【図19】 ルータの構成を機能的に説明するための概念図である。

【図20】 本発明の実施の形態6に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。

【図21】 複数のルータの内部構成を示すブロック図

である。

【図22】 侵入検出部における構造体数検査処理を説明するためのフローチャートである。

【図23】 侵入検出部のアクセス状況返信処理を説明するためのフローチャートである。

【図24】 上述の4つのルータのうち3つのルータの構成を機能的に説明するための概念図である。

【図25】 本発明の実施の形態7に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。

【図26】 本実施の形態7に係る侵入検出部における構造体生成/破棄処理を説明するためのフローチャートである。

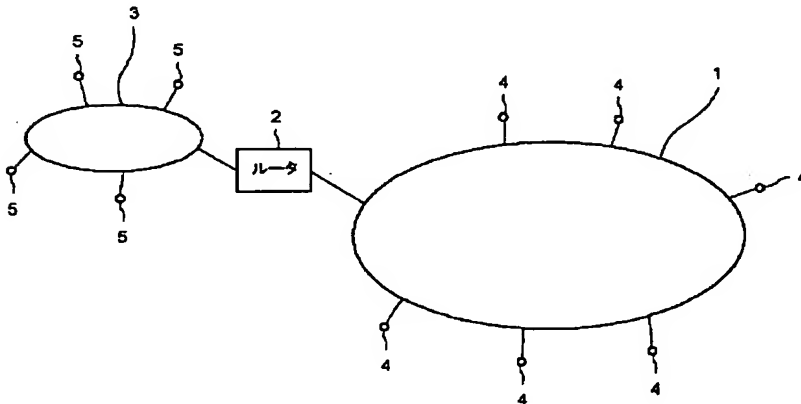
*【図27】 本実施の形態7に係るおとりサーバにおける構造体生成/破棄処理を説明するためのフローチャートである。

【図28】 ルータの構成を機能的に説明するための概念図である。

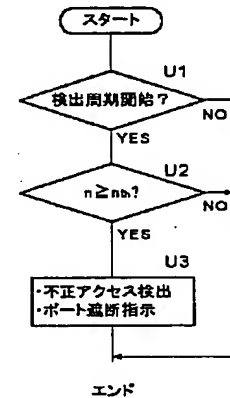
【符号の説明】

1 外部ネットワーク、2 ルータ、3 内部ネットワーク、11 侵入検出部、11a しきい値記憶部、11b 構造体記憶部、21A、21B ルータ、23 上位管理装置、23a 侵入判定部 40A~40D 内部ネットワーク、41A~41D ルータ、43 上位管理装置、50 補正しきい値記憶部、60A~60C ルータ、61A~61C おとりサーバ。

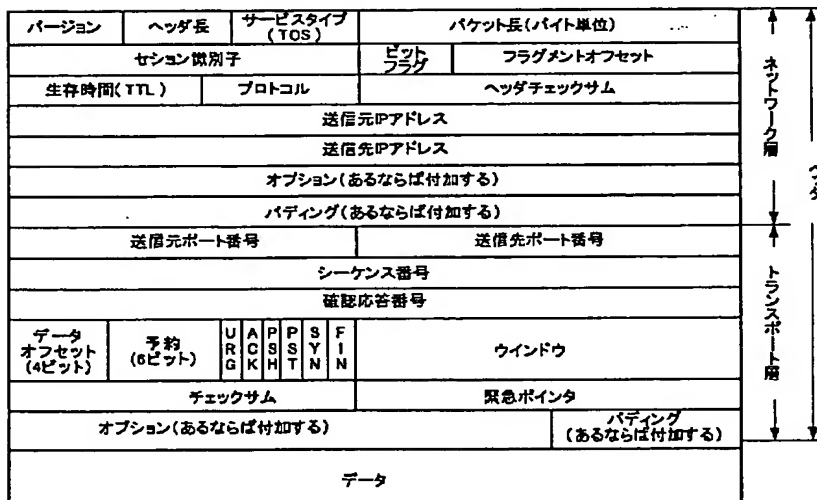
【図1】



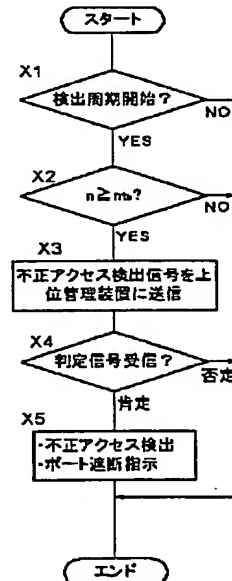
【図7】



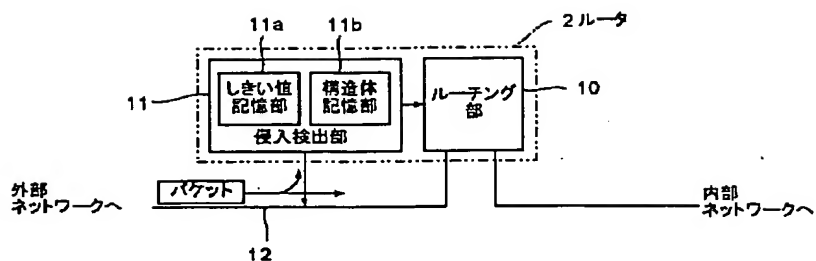
【図2】



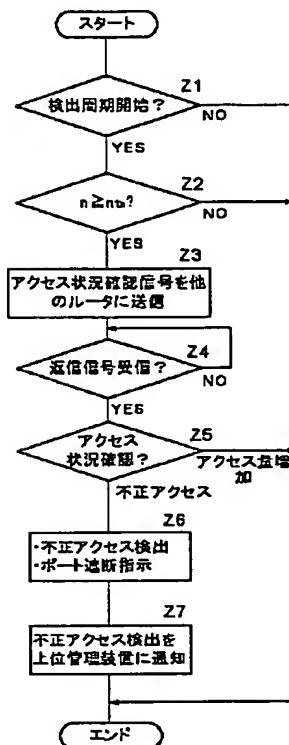
【図14】



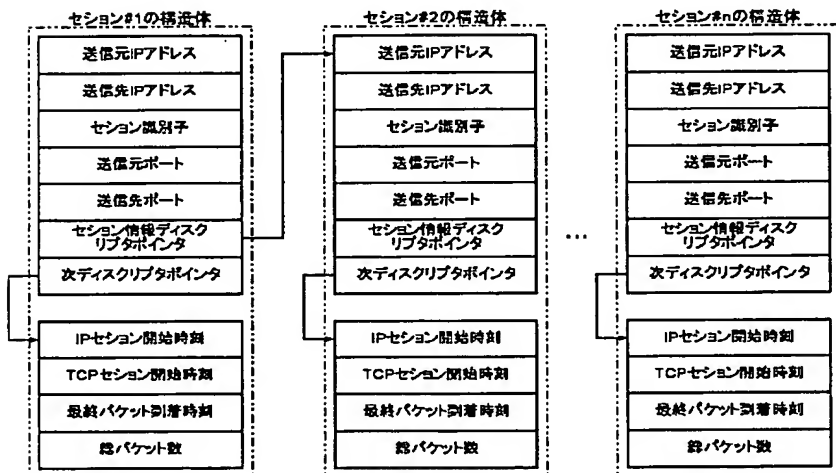
【図3】



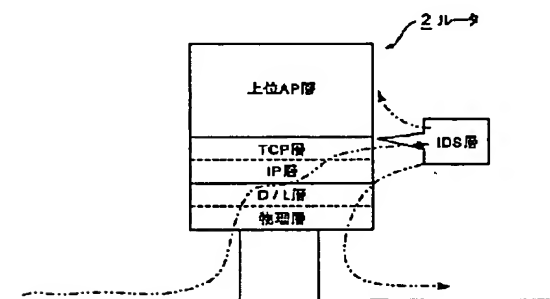
【図17】



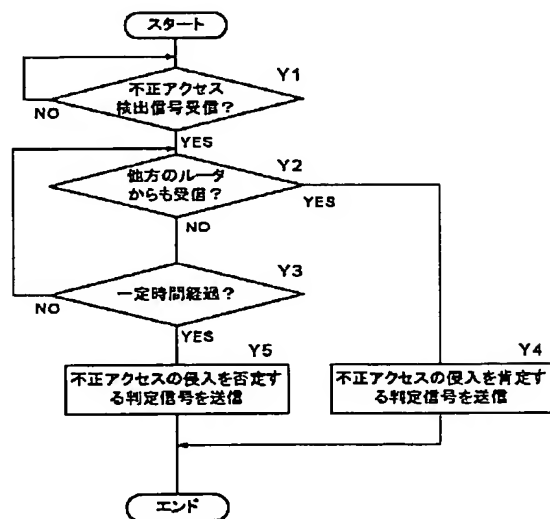
【図4】



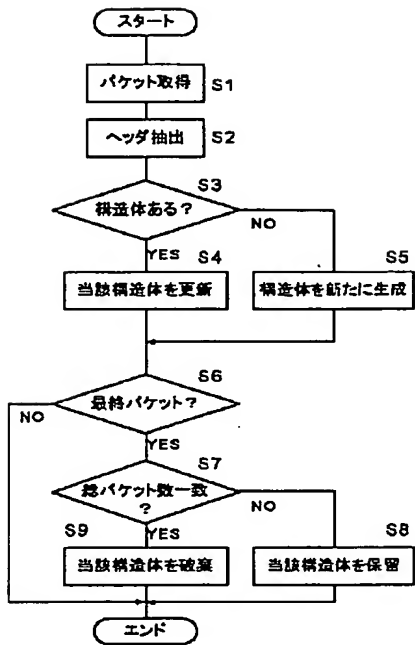
【図10】



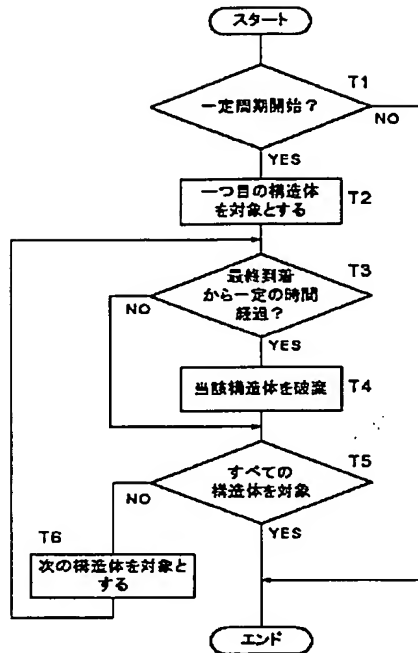
【図15】



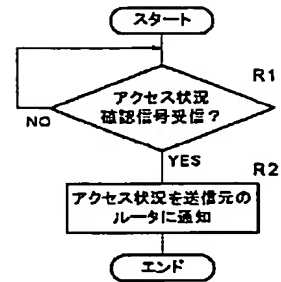
【図5】



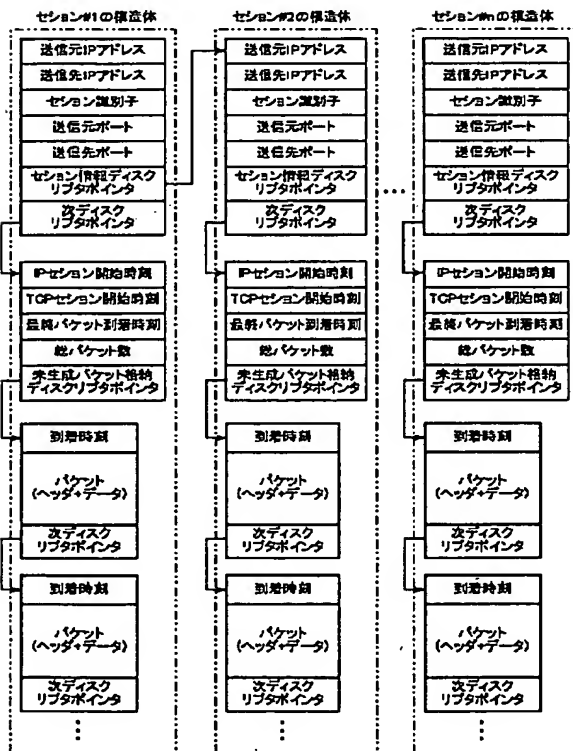
【図6】



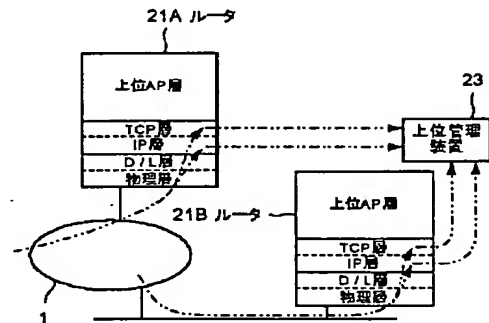
【図18】



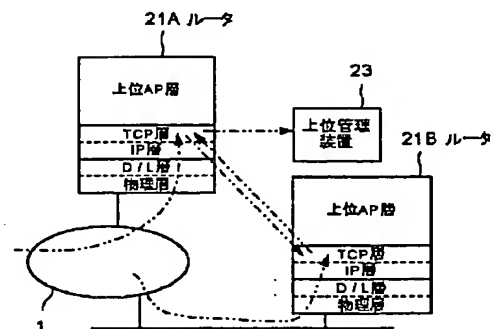
【図8】



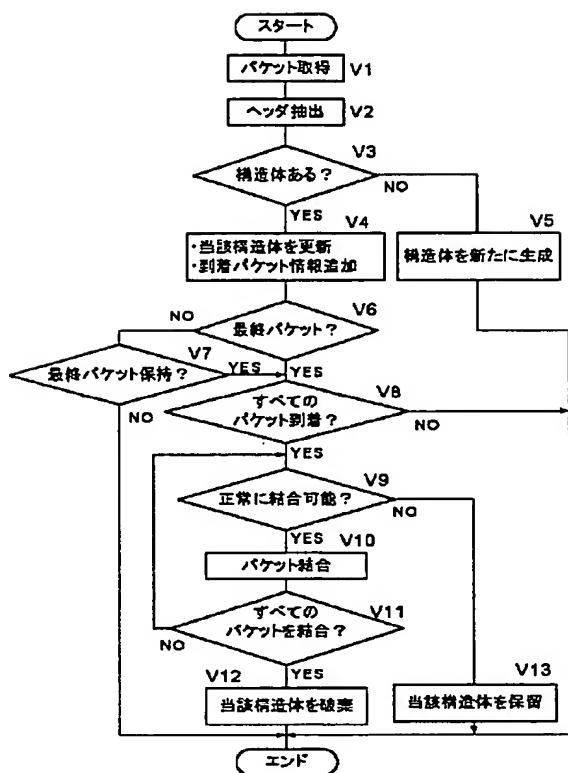
【図16】



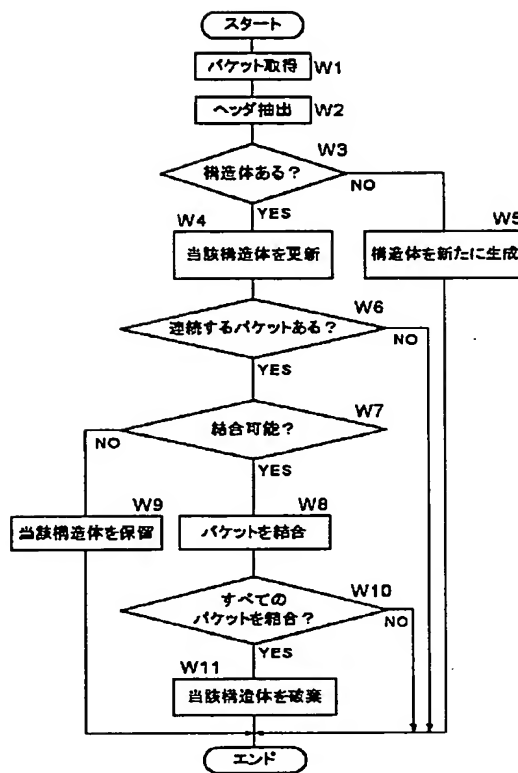
【図19】



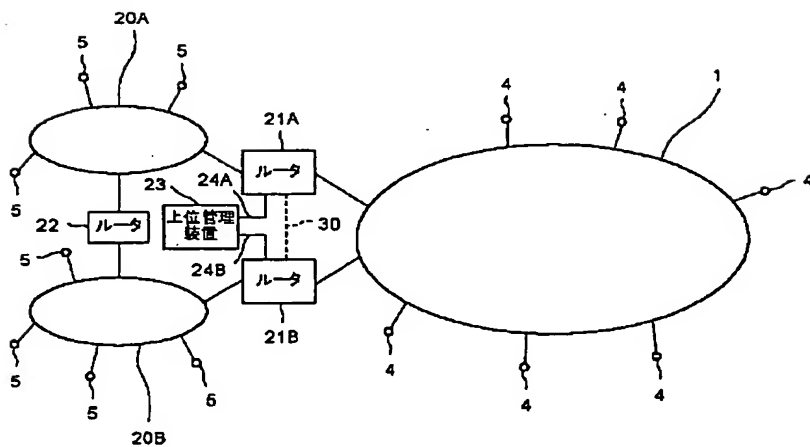
【図9】



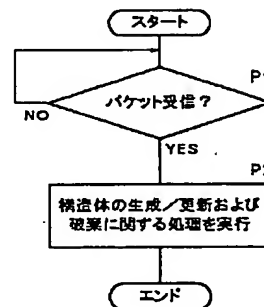
【図11】



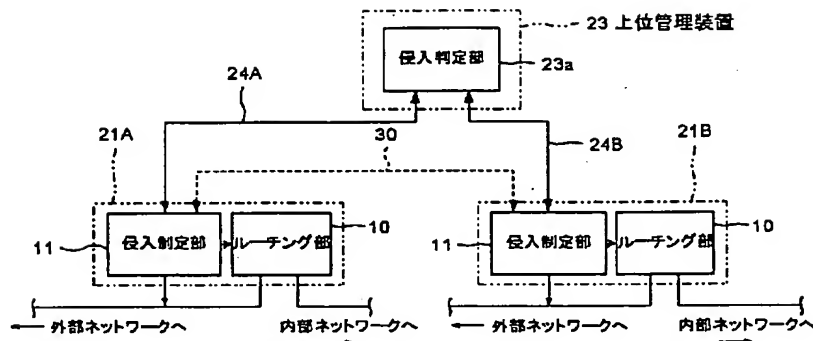
【図12】



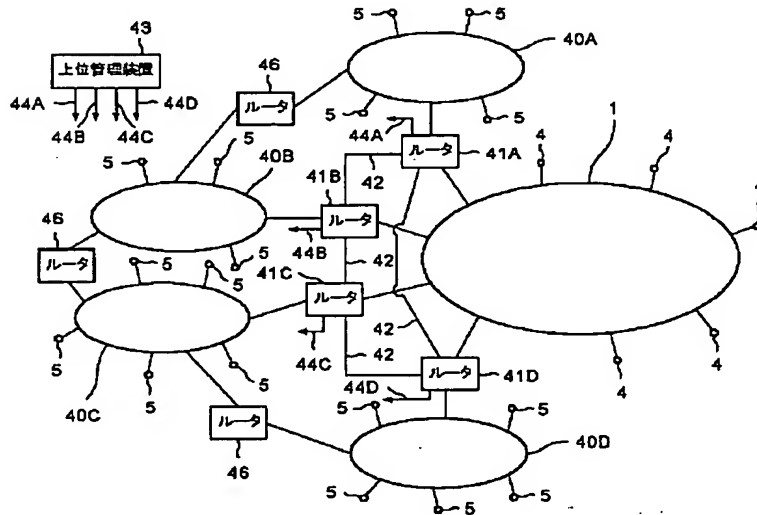
【図27】



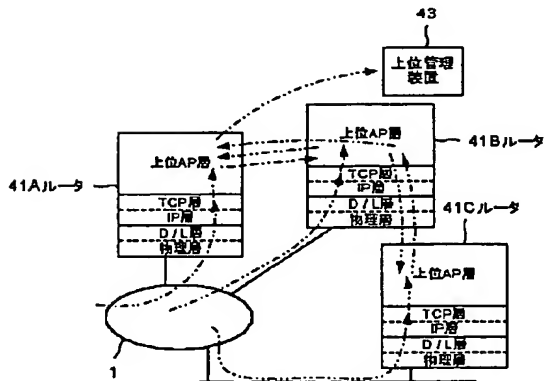
【図13】



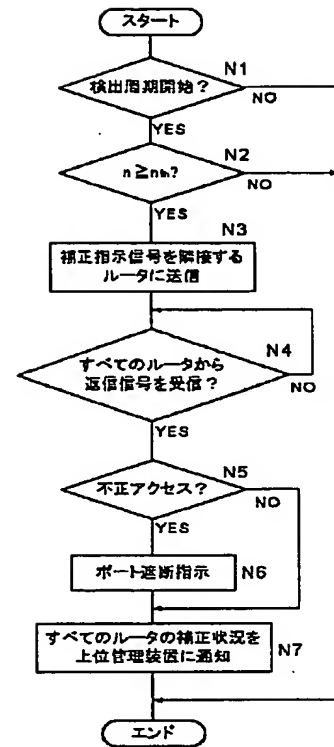
【図20】



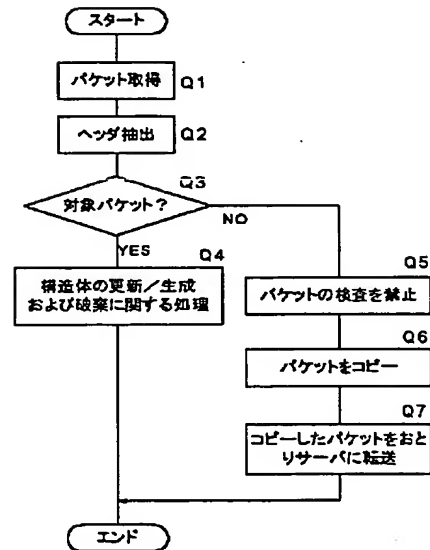
【図24】



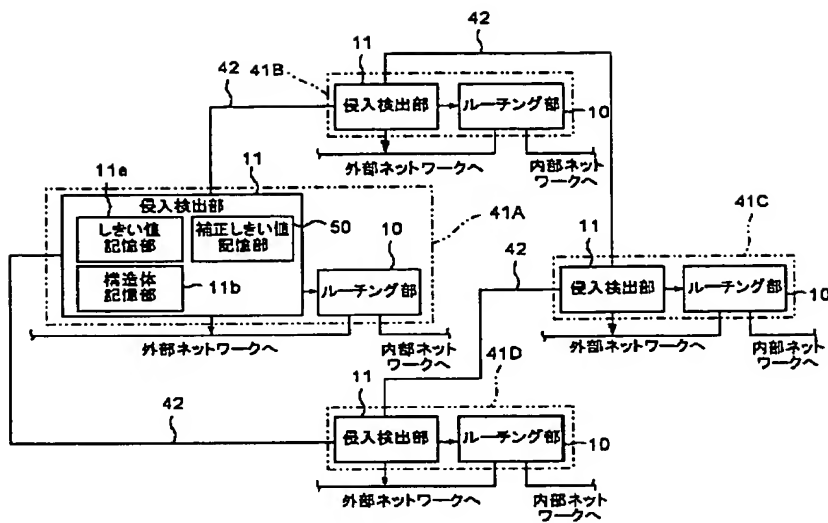
【図22】



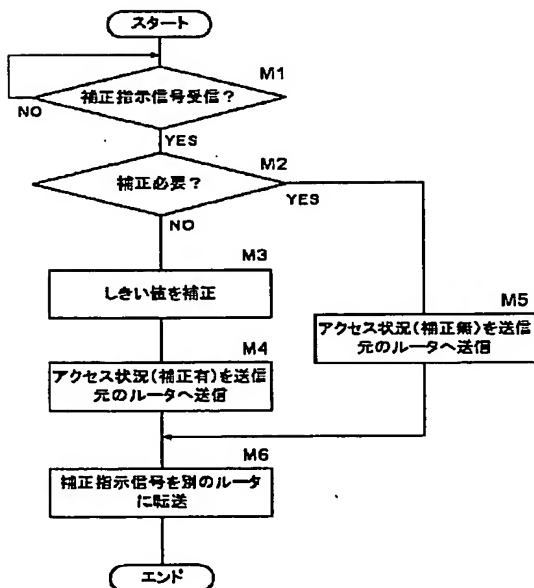
【図26】



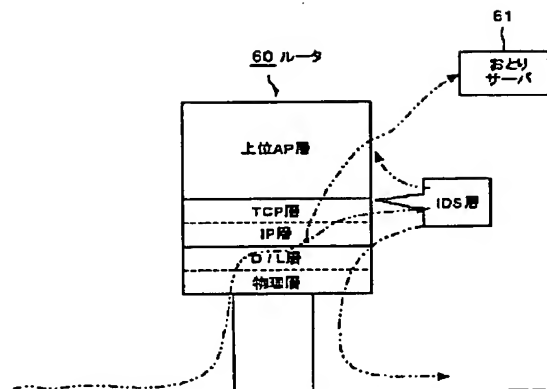
【図21】



【図23】



【図28】



【図25】

